Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Annual 64.2009(e) CPNI Certification for 2011

Date filed: March 1, 2012

Name of company covered by this certification: Envoi USA LLP

Form 499 Filer ID: 826165

Name of signatory: Paul W. Miniotas

Title of signatory: President

I, Paul Miniotas, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq*.

Attached to this certification is an accompanying statement of compliance and the company's Information Security Policy explaining how the company's procedures ensure that the company is in compliance with the requirements, as set forth in section 64.2001 *et seq.* of the Commission's rules

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI , and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed 

Statement of Adherence to CPNI Requirements

- Envoi USA LLP does not make and has never made available to any affiliated or unaffiliated entity information that meets the definition of CPNI set forth in U.S.C. 222(h)(1), except in the provisioning of telecommunications service from which CPNI is derived.

- Envoi USA LLP has been in compliance with the CPNI requirement since January 1, 2007. Although the specific language and policies required by the Code of Federal Regulations are not addressed in our previous Information Security Policy.

- The Envoi Information Security Policy was in place before January 1, 2007 and continues to provide the framework for securing and protecting all of Envoi's customer data.

- The Envoi Information Security Policy has been re-written (as attached below) to ensure the language and procedures are synchronized with the Code of Federal Regulations. Specific procedures and language were added to address the CPNI requirements.

- Envoi has always kept CPNI and other account information confidential and has never received a request to share or disclose CPNI for any person or customer.

- Envoi does not use the CPNI of any customer other than to bill for telecommunications services, and provide inbound administrative services to the customer for the duration of the call.

- No request by any company employee has been made to use or disclose CPNI and no authorization has been given.

- No requests have been made, or approval been given, to employees or affiliates to use marketing or sales campaigns involving the use of CPNI.

Envoi Information Security Policy

Scope of the Information covered by this Policy
This policy is intended to cover any information, in any format, collected by Envoi when providing Envoi VoIP services. The following types of data, include but are not limited to; (1) Customer Proprietary Network Information (CPNI) including any data collected about consumer's telephone calls. Examples include; the time, date, duration and destination number of each call, the network type and the products and services the customer subscribes to. (2) Customer Account details including; Customer Name, address, contact numbers, email address, invoice amounts, payment type, and referral customers. The Safeguard measures taken to protect this data include are categorized in the following; Administrative, Physical, Technical, Organizational and CPNI. A list of additional policies and procedures are included for CPNI access and use.

Administrative Safeguards

Envoi has undertaken administrative measures to appropriately protect the information collected and stored when providing VoIP Telecommunication Services. We require that both the measures taken and documentation of those measures be kept current. This is reviewed and updated periodically so that we continue to appropriately protect the collected and stored data.

1. Security Management Process
The Security Management Process involves the administration, and oversight of policies to address the full range of security issues. This is to ensure the prevention, detection, containment and correction of security violations. This process includes the implementation of features consisting of risk analysis, risk management, and security policies.

2. Assigned Security Responsibility
The responsibility for the Security Management Process has been assigned to a specific individual within our organization to provide focus and priority to the process. Responsibilities include; (1) Supervision of the use of security measures to protect data; (2) Supervision of the conduct of personnel in relation to the protection of data. (3) Training staff in the Information Security Policy; (4) Enforcement of Policies and Procedures; (5) Periodic review and update of the policy

3. Information Access Management
Information Access Control requires the maintenance of formal, documented policies and procedures defining levels of access for all personnel authorized to access any Call Detail, Customer, End User, and Web Portal Login information. Included is how system access credentials are granted, modified and managed.

4. Security Awareness and Training
This policy requires mandatory Security Training for all staff. Training includes; awareness training, periodic security reminders and user education concerning protection from malicious software, the importance of monitoring login success/failure, how to report discrepancies, and password management.

5. Termination Procedures
Envoi's Termination Procedures implement procedures for the ending of an employee's employment or changing an employee's internal or external user access. These procedures include; (1) changing combination locks; (2) removal from access lists; (3) removal of user account(s); and (4) and the return of keys, or cards that allow access to controlled areas.

6. Security Incident Procedures
Security Incident Procedures require formal, documented report and response procedures so that security violations will be handled promptly. We have adopted these procedures as documenting, reporting and responding to incidents are an integral part of our security program.

Physical Safeguards

This section includes features to physically safeguard the data integrity, confidentiality, and availability of the information collected and stored when providing VoIP Telecommunication Services. They include: Facility Access Controls, Server Access Controls, Server Use Policy and Video Surveillance

1. Facility Access Controls - Envoi's Facility Access Controls limit physical access to the location of the technology responsible for providing VoIP Telecommunication Services. These controls consist of procedures and environments for limiting unauthorized physical access, while ensuring that authorized access is allowed. A Photo Security Pass is required for building access. Security personnel checks picture card for match to carrier, for

further building and elevator access. An electronic card swipe in the elevator and server room required to further access the environment. Lastly, there is padlocked access into a caged data locker where the VoIP Telecommunication Technology resides.

2. Server and Switch Access Controls - Each device responsible for providing VoIP Telecommunication Services is secured by a series of physical access control measures. Each server and switch device is protected by a locking, steel chassis with an audible alarm, triggered when the lock is tampered with. Additionally, each server operating system is control locked and secured by a complex password.

3. **Server Use Policy -** We have implemented policies and guidelines on server use delineating the proper functions to be performed and the manner in which those functions are to be performed (for example, logging off before leaving a server unattended). This maximizes the security of collected and stored information.

4. **Video Surveillance -** All areas in the building, elevator, server/network room and cage where the VoIP Telecommunication systems are located are under 24 hr. video surveillance. If any unauthorized access is noticed by the on-site security team, Envoi is notified immediately.

Technical Safeguards

We have incorporated five Technical Safeguards: Technology Access Control; Server Access Audits; Data Integrity Check; and Entity Authentication. Also included are specific technical security procedures for transmitting data over open communication networks, with supported protocols and approved software.

1. Technology Access Control - We have deployed an Access Control System with provisions for context-based, role-based, and/or user-based access. This control includes the unique user identification and password issuing procedures outlined below in Person and Entity Authentication. Additionally, a provision for emergency access procedures and system automatic log-off is included.

2. Server Access Audit - The Server Access Audit is a scheduled, periodic internal audit of all Envoi technology providing VoIP Telecommunication services. This involves a review of: system access, system activity, server logins and file access.

3. Data Integrity Check - This periodic check corroborates Envoi stored data existing in internal databases has not been altered or destroyed in an unauthorized manner. This is achieved through the comparison of stored data to off site back ups and original files, then when required they are cross referenced to server the server access audit results. We have adopted this procedure to ensure that any file corruption or loss that occurs on our internal databases is detected, corrected and reported in a timely manner.

4. Person or Entity Authentication - We have implemented a system for Entity Authentication. This is the corroboration that an entity is who it claims to be. This is accomplished through a system combining unique user identification with a managed password rotation and issuing system.

5. Transmission Security - A set of technical security mechanisms have been deployed to guard against unauthorized access to data that is transmitted electronically, from one point to another, over open communication networks. Our solution requires all transmissions use a Virtual Private Network or alternative encryption technology when transferring data over open networks.

Organizational Requirements

1. Subcontractors and Service Providers - Each Envoi Subcontractor or Service Provider, that has any access to the data covered by this policy, must comply with these security standards to ensure all information and activities are protected from unauthorized access. If the Subcontractor is part of a larger organization, then unauthorized access by that larger organization must be prevented. The agreement between Envoi and a Subcontractor or Service Provider will provide they; (1) implement safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected data it creates, receives, maintains, or transmits on behalf of Envoi; (2) report to Envoi any security incident of which they become aware of.

Customer Proprietary Network Information (CPNI)

CPNI safeguards and procedures are listed separately due to the specific nature in which CPNI is handled, accessed and released. CPNI information is subject to the rules and procedures above in addition to those specifically listed below. A system of clearly identifying the customer's status of CPNI status is in place. All Envoi CPNI is held confidential (Opt-out) until a notice of Opt-In is received and verified.

1. CPNI Opt-In – A status of CPNI Opt-In authorizes Envoi and their affiliates to use the CPNI**.** All Envoi CPNI is held confidential until a notice of Opt-In is received. At the customer's request, a notice of CPNI Opt-In is mailed to the customer at the address of record. No CPNI is authorized to be used until the CPNI Opt-In form is received back to our company, verified and filed accordingly.

2. CPNI Opt-Out - A status of CPNI Opt-Out removes the authorization of Envoi and their affiliates to use the CPNI. When a customer has an Opt-In status and requests the status to be changed to Opt-Out a notice of CPNI Opt-Out is mailed to the customer at the address of record. Upon the Opt-Out request, the customer CPNI is immediately changed to Opt-Out or confidential status and remains as such, even if the completed Opt-Out notice is not received from the customer.

3. CPNI Opt-Out availability - When a customer reports any inability to Opt-Out of CPNI use it must be immediately reported to the company president and in turn a report to the Commission is sent using the format as required in 47 U.S.C. 222 and section 47 C.F.R. 64.2009 (f)(1).

4. CPNI Release Requests - Should any person should contact us and wish to have CPNI released to them, the following methods of verifying the customer identity must be followed before releasing the requested information

i. Customer Initiated Telephone Call

If the request is made by a customer-initiated telephone call, the caller is asked to verify any recent telephone call made from their telecommunications service provided by us, They call detail information must be clearly identified using the telephone number that was called, call date / time and call duration

a. If the customer correctly verifies a past phone number called, call date/time and duration the requested CPNI information will be released.
b. If the caller cannot verify this information the requested CPNI information is not released.

If the caller is unable to verify a call made with the past phone number called, call date/time and duration details there are two options to release the CPNI requested.

1) A call is placed to the customer at their phone number of record and upon verifying the customer request, the requested CPNI information is released
2) A printed version of their requested CPNI can be sent to the customer's address of record.

ii) Customer initiated mail-in request – If the request is made by a customer initiated mail-in request or by email two options to release the CPNI are available:

1) A call is placed to the customer at their phone number of record and upon verifying the customer request, the requested CPNI information is released
2) A printed version of their requested CPNI can be sent to the customer's address of record.

iii). Customer In-Store request – If the request is made by a customer in person in our offices a piece of government issued identification must be produced verifying their identity and address of service before any CPNI is released.

5. CPNI Training - All company personnel have been trained in our Information Security Policy. In addition CPNI training is set out so each employee understands they are not authorized to use CPNI without express written consent of the company president. The president's decision is guided by the Opt-In / Opt-Out status of the customer and rules for use as set out in the Commissions report.

6. Disciplinary Actions - Disciplinary actions for the unauthorized use of customer CPNI include the methods as above in Administrative Safeguards #5 Termination procedures. In addition any unauthorized use of CPNI will result in:

a. A Formal letter of reprimand and non adherence to the company policy is issued to the employee
b. He offending employee is required to re-train in the company Information Security Policy

c. If it is a repeat offence, the employee is immediately dismissed from his job until a review of the circumstances is preformed.

7. Sales and Marketing Campaigns - No company or affiliate will undertake any sales or marketing campaigns that require the use of CPNI. All Sales and Marketing campaigns must be approved by the company president. The decision to approve any sales or marketing campaign is guided by the company's objectives and the rules to use CPNI as described in the Commissions report.